Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-18. (canceled)

19. (currently amended) A group signature ~~system~~device ~~enabling a member (M) of a group (G) to produce~~for providing a message (m) accompanied by a group signature (S), comprising:

~~for proving to a checker (2, 4) that the said message (m) originates from a member (M) of said group (G), using personalized data (z; Kz),~~

~~characterized in that said system is electronic and includes an electronic hardware support (26) and in that the said~~

means for storing personalized data (z, Kz) identifying a member (M) of a group (G);~~is integrated into said electronic hardware support (26)~~ and

means for producing the group signature (S) using the message (m) and the personalized data (z, Kz) such that a checker, upon receiving the message (m) accompanied by the group signature (S), is able to verify that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S), to authenticate the message (m) with the identity of the member (M) of the group (G) remaining anonymous to the checker; and

means for outputting the message (m) and the group signature (S) to the checker.

20. (currently amended) A group signature ~~system~~ device according to claim 19, ~~characterized in that said hardware support includes~~further comprising:

encryption means (B3) for producing personalizing encrypted text (C) using ~~the~~ said personalized data (z; Kz);

said means for producing the group signature (S) being configured to produce ~~before~~ the signature (S) of the message (m) using said personalized encrypted text (C).

21. (currently amended) A group signature ~~system~~ device according to claim 20, further comprising:

~~characterized in that said hardware support further includes~~ means (B5) for combining the message (m) to be signed and the encrypted text (C) associated with said message (m) in the form of a concatenation of the message (m) with the encrypted text (C).

22. (currently amended) A group signature ~~system~~ device according to claim 19, wherein said means for producing the group signature (S) further comprises:

~~wherein the hardware support further includes~~ signature means (Sig-B6) for producing ~~a~~ the group signature (S) of the message (m) ~~with the personalized data (z; Kz) in any~~using the encrypted ~~form~~ text (C) associated with said message (m).

23. (currently amended) A group signature ~~system~~ device according to claim 20, ~~characterized in the~~wherein

said personalized data is an identifier (z) personal to the member (M); ~~, and in that the~~

said ~~electronic hardware support (26)~~ means ~~-~~for storing further includes an encryption key (K) common to all members of the group (G);[[,]] and

encryption means (B3) ~~for encrypting~~produces said encrypted text (C) using the identifier (z) ~~with the~~and said encryption key (K).

24. (currently amended) A group signature ~~system~~ device according to claim 23, ~~characterized in that~~in which encryption means (B3) produces said encrypted text ~~encrypts the text~~ (C) ~~with~~ using the identifier (z) and a random number (r).

25. (currently amended) A group signature ~~system~~ device according to claim 20, ~~characterized in that the~~wherein

said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G);[[,]] and

~~in that~~ encryption means (B3) produces said encrypted text ~~encrypts the text~~ (C) using at least one data ~~(r) with the~~and said diversified encryption key (Kz).

26. (currently amended) A group signature ~~system~~ device according to claim 25, ~~characterized in that the~~wherein said data ~~(r)~~ includes a random number (r).

27. (currently amended) A group signature ~~system~~ device according to claim 24, ~~characterized in that~~wherein the encryption means (B3) uses a secret key (K) and the Advanced Encryption Standard (AES) public encryption algorithm ~~(K)~~.

28. (currently amended) A group signature ~~system~~device ~~hardware support~~ according to claim 26, wherein the encryption means (B3) ~~use either a~~uses one of the Rivest, Shamir, Adleman ~~public key encryption algorithm RSA (Rivest, Shamir, Adleman)~~(RSA) or ~~an AES (~~the Advanced Encryption Standard (AES) public encryption algorithms.

29. (currently amended) A group signature ~~system~~ device according to claim 22, ~~characterized in that~~wherein the signature means (Sig-B6) uses a private key signature algorithm (SK).

30. (currently amended) A group signature ~~system~~ device according to claim 29, ~~characterized in that~~in which the private key signature algorithm is of the Rivest, Shamir, Adleman (RSA) type ~~(Rivest, Shamir, Adleman)~~.

31. (currently amended) A group signature ~~system~~ device according to claim 19, ~~characterized in that said hardware support comprises~~in which said group signature device is a portable communicating device ~~(26)~~.

32. (currently amended) A group signature ~~system~~ device according to claim 31, ~~characterized in that~~in which said portable communicating device is a smart card ~~(26)~~.

33. (currently amended) A method for secure communication of ~~checking~~ a message (m) sent by a member (M) of a group (G) ~~accompanied by a~~using a group

signature (S), ~~wherein the message (m) authentication the signature to indicated that the message originates from a member of the group, comprises~~comprising:

producing the group signature (S) of the message (m) with a private key (SK) common to members (M) of the group (G); ~~and~~

integrating personalized data (z; KZ) ~~electronic hardware support (26)~~ into the message (m);[[,]] and

~~transmitting~~ outputting the message (m) along with the ~~authenticated~~ group signature (S) ~~to a user of the system (2,6)~~; and

verifying that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S) to authenticate the message (m) without identifying the member (M) of the group (G) ~~without needing to supply proof to the user that the member (M) belongs to the said group (G)~~.

34. (currently amended) ~~A method for checking a message (m) sent~~The method according to claim 33, ~~characterized in that the message is checked~~in which said verifying is performed using a public key corresponding to ~~the~~ said private key (SK).

35. (currently amended) ~~A method for opening a signature (S) produced by a group signature system which enables a member (M) of a group (G) to produce a message (m) accompanied by the signature (S) so as to authenticate the signature (S) for a user of the system~~ The method according to claim 33, further comprising the steps of:

making correspondence data between the identities of members (M) of the group (G) and their personalized data available, before ~~the~~ said producing the group signature(S);

decrypting the personalized data received from an electronic ~~hardware support (26)~~device for which the group signature (S) is to be opened; and

opening the group signature (S) ~~when~~if the decrypted personalized data corresponds to the identity of the member (M) of the group (G).

36. (currently amended) ~~A method for adapting an electronic hardware support (26) for a group signature system which enables a member (M) of a group (G) to produce a message (m) accompanied by a signature (S) to authenticate the signature (S) for a user of the system wherein the hardware support is personalized to a member (M) of the group, characterized in that it comprises~~The method of claim 35, further comprising the steps ~~consisting~~ of:

producing personalized data ~~(z; Kz)~~(z, Kz) ~~to be used for the~~associated with said electronic ~~hardware support (26)~~device to be personalized; and

registering ~~this~~ said personalized data (z, Kz) with a private signature key (SK) ~~in the said hardware support~~contained in said electronic device.

Claims 37-38. (canceled)

39. (new) A group signature system for authenticating a message (m) accompanied by a group signature (S), comprising:

an electronic device configured to store personalized data (z, Kz) identifying a member (M) of a group (G), to produce the group signature (S) using the message (m) and the personalized data (z, Kz), and to output the message (m) and the group signature (S);

a checker that receives the message (m) accompanied by the group signature (S) output from the electronic device, said checker being configured to verify that the message (m) is associated with the group (G) based on the personalized data (z, Kz) and the group signature (S), the identity of the member (M) remaining anonymous to the checker; and

a trusted authority configured to identify the member (M) of the group (G).

40. (new) A group signature system according to claim 39, further comprising:

a terminal including means for communicating with the electronic device; and

a server provided in communication with the terminal and the trusted authority;

wherein said trusted authority is provided in communication with a bank and a shopkeeper.